10

20

25

What we claim is:

1. In an infrastructure in which some of a plurality of entities provide cryptographically supported services, a method of registering a subscriber entity of a plurality of entities at a principal entity of a plurality of entities, the method comprising:

the subscriber entity requesting service from the principal entity by sending a request message to a registrar entity of the plurality of entities;

the registrar entity verifying the subscriber entity and forwarding the request for service to the principal entity;

the principal entity storing the forwarded request and transmitting an acknowledgement message to the registrar entity, the acknowledgement stating acceptance and authentication/authorization information that the subscriber entity requires for the requested service; and

the registrar entity verifying the authenticity of the received acknowledgement message, and, if correct, forwarding the acknowledgement message to the subscriber entity.

- 2. A method as in claim 1 wherein the request message contains an indication of the type of service requested by the subscriber entity.
 - 3. A method as in claim 2 wherein the request message contains one or more of the following:
 - (a) a unique reference to the subscriber entity;
 - (b) attributes about the subscriber entity;

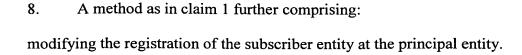
10

15

- (c) authentication information to be used to authenticate use of the service;
- (d) transactional verification information;
- (e) representations by the subscriber entity agreeing to what the subscriber accepts;
- (f) preferred service relationships;
- (g) a subscriber's authenticator.
- 4. A method as in claim 3 wherein the unique reference to the subscriber is at least one of (a) the subscriber's identity, (b) a pseudonym for one-time service, and (c) a pseudonym for continued use of the service
- 5. A method as in claim 3 wherein the session identifier links future responses to this particular request.
- 6. A method as in claim 3 wherein the attributes about the subscriber include:
 - (a) self-representations; and
 - (b) third-party representations asserting attributes.
- 7. A method as in claim 6 wherein said representations and attributes include at least some of:
 - (a) addresses;
 - (b) employment information;
 - (c) information from other entities needed for service provisioning; and
 - (d) authorizations from other parties.

10

20



- A method as in claim 1 further comprising:
 moving the registration for service from the principal entity to another entity
 of said plurality of entities.
- 10. A method as in claim 1 wherein the service includes: operating cryptographically-supported transaction involving the subscriber entity, the principal entity and possibly additional entities.
- 11. A method as in claim 1 wherein the subscriber entity comprises a plurality of elements.
- 12. A method as in claim 11 wherein the plurality of elements are associated with an entity.
- 13. A method as in claim 1 where said service is a subset of a totality of services.
 - 14. A method as in claim 1 where service is a warranty service.
- 15. A method as in claim 13 wherein another subset of the totality of services to the subscriber entity is provided by an entity different from principal entity.

10

15

20

- 16. A method as in claim 15 wherein the subscriber entity can modify the subset of totality of services between entities.
- 17. A method as in claim 8 where modification is supervised by authorities.
- 18. A method as in claim 9 where moving of services is supervised by authorities.
- 19. A method as in claim 1 where provision of service may involve additional entity from the said plurality of entities.
- 20. A method as in claim 19 where provision of service is split between said principal entity and said additional entity.
- 21. A method as in claim 1 wherein provision of service by said principal entity on behalf of said subscriber entity is given by said operating infrastructure to an entity within said plurality of entities.
- 22. A method as in claim 1 wherein said provision of service by said principal entity involves other entities within said plurality of entities.
- 23. A method as in claim 14 wherein said warranty service involves correctness of representation of information.

10

15

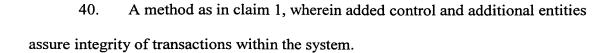
20

- 24. A method as in claim 23 wherein said representation of information is at least one of: (a) identity information, (b) financial information; (c) information derived from provision of service within said infrastructure.
- 25. A method as in claim 14 wherein the system includes a mechanism to initiate claims against failed warranty.
- 26. A method as in claim 1 wherein said service provision involve control of access.
- 27. A method as in claim 1 wherein at least one of said plurality of entities is an enterprise.
- 28. A method as in claim 1 wherein at least one of said plurality of entities is a financial institute.
- 29. A method as in claim 1 wherein said principal entity is a group of elementary entities.
- 30. A method as in claim 1 wherein said provision of service by principal entity is directed by said subscriber entity.
- 31. A method as in claim 8 wherein registration modification transactions involve managing capabilities.

20

- 32. A method as in claim 8 wherein registration modification transactions involve cryptographic key management.
- 33. A method as in claim 1 further comprising:

 providing, by the principal entity, at least one of a set of various service transactions to the subscriber entity.
- 34. A method as in claim 33 wherein said providing involves the certification of digital identities.
- 35. A method as in claim 33 wherein at least one of said service transactions involves assuring an entity's state.
- 36. A method as in claim 33 wherein at least one of said service transactions involves assuring financial information.
- 37. A method as in claim 33 wherein at least one of said service transactions involves assurance of identity and assurance of entity's state.
- 38. A method as in claim 1 where some of said plurality of entities are supervised by other entities in at least one transaction.
 - 39. A method as in claim 1, where services involve fees based on service agreements and contracts.



- 41. A method as in claim 40 wherein the integrity of the management function is enhanced by providing two or more independent reports.
- 42. A method as in claim 40 wherein the management function controls actions of assurance offering entities on a per transaction basis.